CITY OF SAN ANTONIO

Administrative Directive	**7.4 Acceptable Use of Electronic Communications**
Procedural Guidelines	Policy and procedures applicable to the use of electronic communications systems
Department/Division	Information Technology Services Department
Effective Date	October 1, 2012
Project Manager	_____, ITSD

Purpose

This Administrative Directive provides guidance for the use of electronic communications systems, including electronic mail and internet access, operated and maintained by the City of San Antonio. This Directive supports and supplements Administrative Directive 7.5- Acceptable Use of Information Technology. This directive does not supersede provisions of Directive 7.5.

Policy

The City of San Antonio provides e-mail services and internet access to its employees as tools to perform business-related activities. All users of the City's electronic communications systems, including its internet access facilities, are responsible for using that technology in an appropriate and lawful manner. Any activity performed on a workstation under an employee's login ID is presumed to be performed by that employee and is the responsibility of the employee.

The City manages its electronic mail records in accordance with Texas Administrative Code, Chapter 7, Sections 7.71-7.79 and Local Government Code, Chapter 205, Sections 205.001-205.009 (Local Government Bulleting, B, Electronic Records Standards and Procedures).

Most e-mail messages are not essential to the fulfillment of statutory obligations or to the documentation of the city's functions and may be deleted. These messages may include personal messages, internal meeting notices, letters of transmittal, and general FYI announcements.

Messages which do fulfill statutory obligations or document the City's functions are subject to retention and disposition requirements established by the Texas Administrative Code.

The City's internet connection is a shared resource that serves all of its employees and provides the general public with access to its website. Inappropriate use of internet resources reduces the usefulness of this resource to its employees and citizens.

City electronic mail and internet systems are for official business use. Users may make and receive personal communications during business hours that are necessary and in the interest of the City. While some incidental use (as defined in AD 7.5) of City- managed technology is unavoidable, such incidental use is not a right, and should never interfere with the performance of duties or service to the public.

Policy Applies To

☐ External & Internal Applicants	☒ Current Temporary Employees

☒ Current Full-Time Employees	☒ Current Volunteers
☒ Current Part-Time Employees	☒ Current Grant-Funded Employees
☒ Current Paid and Unpaid Interns	☐ Police and Fire Academy Trainees
☐ Uniformed Employees Under Collective Bargaining Agreements	

Definitions	
Electronic mail record	An electronic government record sent and received in the form of a message on an electronic mail system of a government, including any attachments, transmitted with the message.
Local Government Record Retention Schedules	Publications issued by the Texas State Library and Archives Commission under the authority of Subchapter J, Chapter 441 of the Government Code which establish the mandatory minimum retention period for a local government record.
Records Management Officer	The person who administers the records management program established in each local government under Local Government Code, Chapter 203, Section 203.026.
Retention Period	The minimum time that must pass after the creation, recording or receipt of a record or the fulfillment of certain actions associated with a record, before it is eligible for destruction.

Policy Guidelines

This directive applies to all users of the City's electronic mail and internet access systems that connect to the City's network in order to use those facilities. All electronic messaging equipment or technology that is owned or administered by the City is included within this Directive's scope.

Roles & Responsibilities

Information Technology Services Department:

1. Organizational responsibility for the development, implementation, maintenance, and compliance monitoring of this directive is placed with ITSD and the City Clerk's Office.

2. ITSD and Human Resources will provide City departments with initial communication and training regarding application of this directive. However, City Department Directors are ultimately responsible for communicating the policies and standards established in this AD to all personnel in their respective departments and for ensuring compliance within their respective departments with those policies and standards.

3. ITSD is responsible for communicating the policies and standards established in this directive to all third-party users (contractors, consultants, agencies having a contractual relationship with the City) and for ensuring their compliance. Those City departments who work with the third-party users are responsible for identifying the third-party users to ITSD.

4. ITSD will archive undeleted messages after 90 days.

5. ITSD may terminate e-mail services to any user if he/she is found in breach of this directive. Service may be restored to the employee following a written request by the employee's Department Director.

6. ITSD may isolate a sender's email messages from reaching a user's city e-mail account. The following process must be followed in order to isolate email messages sent to the City's technology system:

   a. A user who receives repeated or multiple unsolicited, unacceptable annoying, alarming, abusive, embarrassing or offensive e-mail messages from a sender outside of the City must ask the sender to stop sending such messages and inform the sender that any e-mailed requests for city records or documents must be sent to the City's Officer for Public Information at http://www.sanantonio.gov/opengovernment/.

   b. The user must provide copies of the messages and all correspondence between the user and sender, to the user's supervisor, Department Director, or appropriate Executive Leadership Team member along with a written request to have ITSD isolate the sender's e-mails.

   c. The Department Director or Executive Leadership Team member, the Office of the City Attorney, Department of Communications and Public Affairs, and ITSD will review the request and determine whether the request warrants isolation or other disposition of the e-mails.

Office of the City Clerk:

In cooperation with the ITSD, the Records Management Officer will ensure that appropriate training and communication of the requirements for retention, maintenance, and disposition of records is made available for staff.

Department Directors and their Designees:

1. Departments are responsible for implementation, training, and enforcement of the data classification standards defined by the Texas State Attorney General's Office as they apply to information stored on City-administered technology or equipment including data retention and disposition.

2. Department Directors are responsible for any disciplinary actions taken against employees who violate this policy. The Human Resources Department will provide guidance as required to City departments regarding appropriate disciplinary actions to be taken against employees who violate this policy.

Employees:

1. Employees shall, with guidance and training from the Records Management Officer, manage e-mail messages according to the City's approved retention periods.

2. Employees who voluntarily terminate employment, retire, or are transferred, will be required to review their e-mail accounts with their supervisor. The employee's supervisor is responsible for ensuring that e-mail records are properly classified and stored. All unnecessary working or convenience copies shall be disposed of in the prescribed manner.

Human Resources:

1. Human Resources will provide guidance to departments for disciplinary actions associated with violations of the directive.
2. Human Resources will assist ITSD in providing training regarding this directive to current and future employees. Following implementation of this directive, Human resources will ensure that all new employees are

provided a copy of this directive.

3. The Human Resources Director will consult with the Chief Information Officer in approving any monitoring of systems for personnel reasons.

Procedures

1. All electronic mail messages sent, received, or stored on the City's systems are considered City property and may be read at any time. Messages may be furnished to third parties in order to comply with requirements of the Texas Public Information Act. All internet activity is logged, and logs may be inspected at any time.

2. Security and proprietary information

   a. The use of HTML formatting for e-mail messages is prohibited.

   b. E-mail attachments that may constitute a risk to the City's technology environment will be removed from e-mail messages passing through the City's mail servers. Removed attachments are replaced by a message indicating that they have been removed and the header and text of the original message delivered normally.

   c. A spam message filter is used to reduce the transmission of chain letters, broadcast announcements, general advertisement postings, or any other message via e-mail to a group of persons not requesting the message.

3. The following activities are prohibited unless performed in the course of legitimate job responsibilities. The list below is by no means exhaustive, but provides a framework for activities which fall into the category of unacceptable use:

   a. Engaging in any activity that is illegal under local, state, and/or federal statutes as well as any activity that violates City of San Antonio policies and Administrative Directives.

   b. Using, accessing, or transmitting pornographic or sexually explicit materials, offensive, threatening, racial or hate language or images.

   c. Engaging in any form of harassment, whether sexual or otherwise, or sending any unwelcome personal communication. It is the perception of the recipient that prevails in most instances, not the intent of the sender.

   d. Any personal use that interrupts City business and that keeps an employee from performing his/her work. Employees should not use their City electronic mail account as their primary personal e-mail address.

   e. Extensive personal use of the internet for any non work-related purpose during working hours which decreases the employees productivity or results in decreased performance of the City's internet facilities.

   f. Unauthorized downloading of and distributing of copyrighted materials.

   g. Downloading or copying music, photographs, or video material, including such material that has been obtained legally, onto City computers or servers.

   h. Downloading and/or installing executable program files from the internet without the approval of ITSD.

   i. Unauthorized reading, deleting, copying, modifying, or printing electronic

communications of another user.

j. Using the City's electronic mail or internet systems for private gain or profit.

k. Using personal software which allows peer-to-peer communications between two workstations (eg., online chat, KaZAA, etc.).

l. Using instant messaging through public service providers.

m. Using City systems for personal access to auctions (such as e-Bay).

n. Soliciting for political, religious, or other non-business uses not authorized by the City.

o. Accessing non-business related streaming media, including internet-based radio.

p. Accessing any non-business related application which maintains a persistent connection to the internet, such as "Weather Bug", stock tickers, etc.

q. Using City electronic mail or internet facilities for political purposes, including voting. (This does not include the use of equipment for public voting at City facilities).

r. Including email "tag lines" or personal quotations other than ones that state the mission of the City or the user's Department.

s. Sending or forwarding junk e-mail, chain letters, or other mass mailings.

t. Sending or receiving e-mail through non-City managed e-mail systems (e.g. Hotmail or Yahoo) while at work.

Retention and Disposition of E-mail

The City's approved Declaration of Compliance with the Local Government Records Retention Schedules establishes record series and the retention period for each series. It is the content and function of an e-mail message that determines the retention period for that message. All e-mail sent or received by a government is considered a government record. Therefore, all e-mail messages must be retained or disposed of according to the City's retention requirements. E-mail systems must meet the retention requirement found in Texas Administrative Code, Chapter 7, Section 7.77.

Employees and their supervisors should seek guidance from the City's Records management Officer if there is a question concerning whether an electronic message should be deleted.

Privacy and Monitoring

1. The City does not routinely monitor the content of electronic communications systems, but may do so without notice. City systems may be monitored to support operational, maintenance, auditing, security and investigative activities, including enforcement of this Directive, legal requests, public records requests, or other business purpose. ITSD staff may monitor network infrastructure, servers, and workstations for the purpose of maintaining system reliability, availability, and security.

2. Only Department Directors or higher may request access and monitoring of City administered technology or communications systems for employees under their supervision. Unauthorized monitoring or reading of electronic communications systems or their contents violates this Directive.

3. Any request to monitor must be approved by the Chief Information Officer (CIO) and the Human Resources Director prior to the commencement of monitoring.

4. To obtain the necessary authorization, a written request from the requestor to the Human Resources Director must include:

   a. The stated purpose for accessing and/or monitoring.

   b. A specific description of the systems or content to be accessed and/or monitored (e.g. the name of the mailbox earmarked to review-exactly as it appears in the e-mail directory).

   c. Name and phone number of the employee in the requesting department who is responsible for coordination of the request.

5. The Human Resources Director will forward the request to the CIO for concurrence.

6. The CIO will assign staff from ITSD to assist as necessary with any authorized access and monitoring activities.

Internet Filtering and Waiver Requests

The City uses filtering software to block access to certain internet sites that have been determined by the Management Team to be inconsistent with most employee job responsibilities and other City policies. There may be specific circumstances in which blocking is too restrictive to allow an employee or group of employees to adequately perform their duties. In these cases, a waiver from the policy must be requested. To request a waiver:

1. Employee should complete the on-line site access request form that is available when attempting to access a blocked site.

2. The Chief Information Officer or his designee will review the request in a timely manner, and will verify the business need with the employee's Department Director or Management Team member as may be appropriate. The Chief Information Officer may request guidance from Human Resources and/or Legal Departments as may be necessary.

3. The approved request will be maintained by ITSD.

4. If the requested access will allow an employee to perform activities which are normally prohibited by City policies, the employee's Department Director must submit a request for waiver in writing to the Chief Information Officer. The waiver request must include a statement that the Department Director is aware of any increased risks that will result from the waiver, and has added appropriate mitigating and/or compensatory controls to adequately reduce the additional risks.

Discipline

1. Failure to comply with this directive will result in disciplinary action in accordance with the Municipal Civil Service Rules of the City of San Antonio, Rule XVII, Section 2. Discipline will be evaluated and based upon the number of violations and severity of the incident. The Human Resources Department must be consulted by a department when assessing the appropriate level of disciplinary action.

2. Employees who fail to follow and administer this directive will be disciplined under the authority of the Department Director.

3. This Administrative Directive does not supersede the Department Director's authority over the determination of formal disciplinary actions taken, particularly in cases where the safety of the general public or City employees are significantly compromised by an infraction of this Administrative Directive. A Department Director may choose to assess more severe disciplinary action against an employee depending on the severity of the infraction.

This directive supersedes all previous correspondence on this subject. Information and/or clarification may be obtained by contacting the Information Technology Services Department at 207-8301.

CITY OF SAN ANTONIO

EMPLOYEE ACKNOWLEDGMENT FORM
FOR
ADMINISTRATIVE DIRECTIVE 7.4
Acceptable Use of Electronic Communications

Employee:

I acknowledge that on _____, 20____, I received a copy of Administrative Directive 7.4 Acceptable Use of Electronic Communications. I understand if I should have any questions I should contact my Human Resources Generalist.

_____ _____
Employee Name (Print) Department

_____ _____
Employee Signature SAP ID#